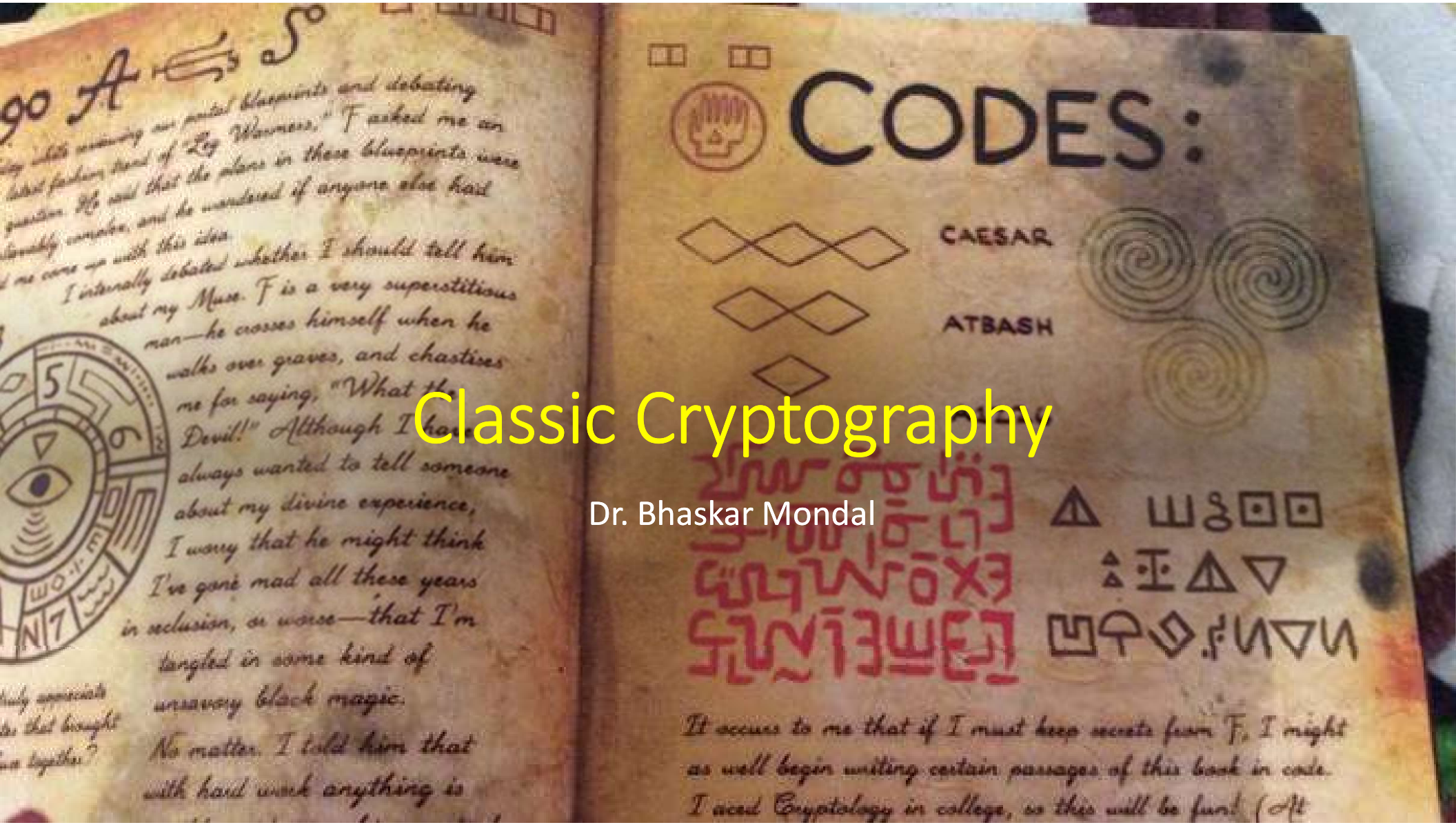
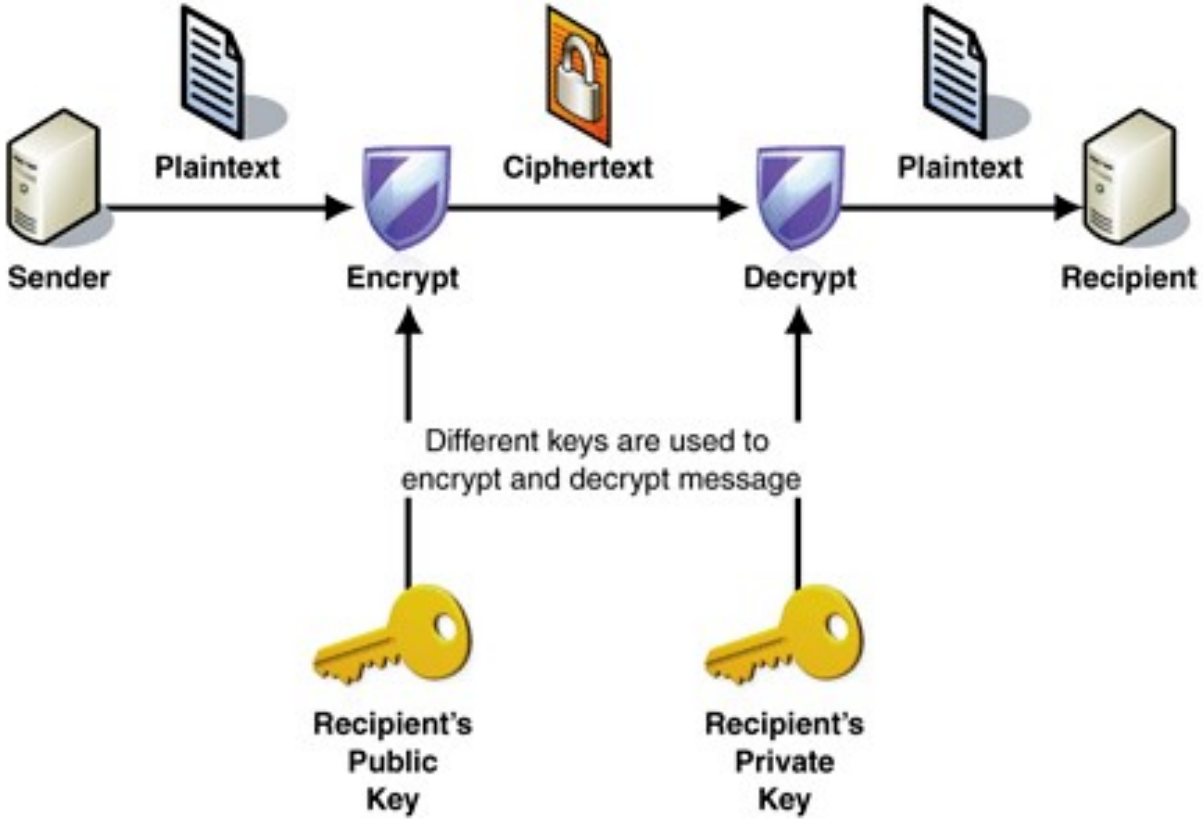

CODES:
CAESAR
ATBASH
Classic Cryptography
Dr. Bhaskar Mondal



Components of a Cryptosystem

Ancient Ciphers

- 3100 B.C ancient Egyptians enciphered some of their *hieroglyphic* writing on monuments
- 100 BC years ago Julius Ceasar used a simple substitution cipher, now known as the **Caesar cipher**
- 1200: Roger Bacon described several methods
- 1392: Geoffrey Chaucer included several ciphers in his works
- 1460s: Leon Alberti devised a **cipher wheel**, and described the principles of frequency analysis
- 1553: Vigenère invented by Giovan Batista Belaso
- 1585: Blaise de Vigenère published a book on cryptology, and described the **polyalphabetic substitution cipher**

Classical Cryptographic Techniques

have two basic components of classical ciphers: substitution and transposition

substitution ciphers: letters are replaced by other letters

transposition ciphers: the letters are arranged in a different order these ciphers may be:

monoalphabetic - only one substitution/ transposition is used, or

polyalphabetic - where several substitutions/ transpositions are used

several such ciphers may be concatenated together to form a **product cipher**

Substitution Cipher: Atbash

- Alphabets are reversed
- P**la**in Text: This is a Cipher
- Cipher Text: Gsrh Rh Z Xrksvi

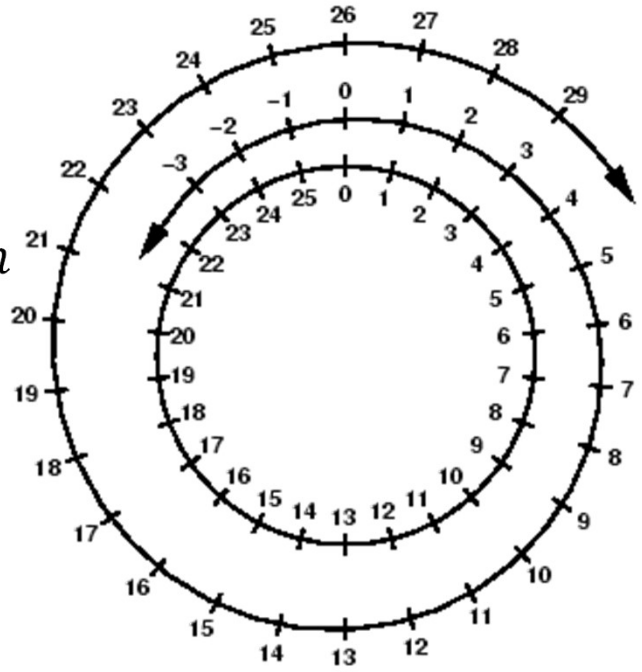
Shift Cipher: Caesar Cipher

- a monoalphabetic Cipher
- reputedly used by Julius Caesar
- replace each letter of message by a letter a fixed distance away e.g. use the 3rd letter on
- $E_n(x) = (x + n) mod\ 26$
- $D_n(x) = (x - n) mod\ 26$

- Text : ATTACKATONCE
- Shift: 4
- Cipher: EXXEGOEXSRGI

Modular Arithmetic monoalphabetic cipher

- If $a \bmod n = b \bmod n$ then there is an integer k
  - such that $a - b = k \cdot n$
- $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
- $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$
- $-a \bmod n = n - (a \bmod n)$

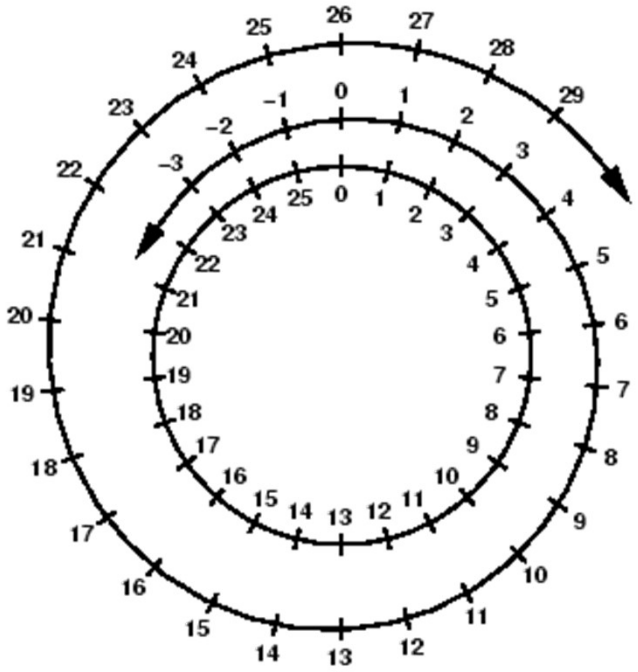


Modular Arithmetic monoalphabetic cipher

- If $a \; mod \; n \; = \; b \; mod \; n$ then there is an integer k
  - such that $a \; - \; b \; = \; k \; \cdot \; n$

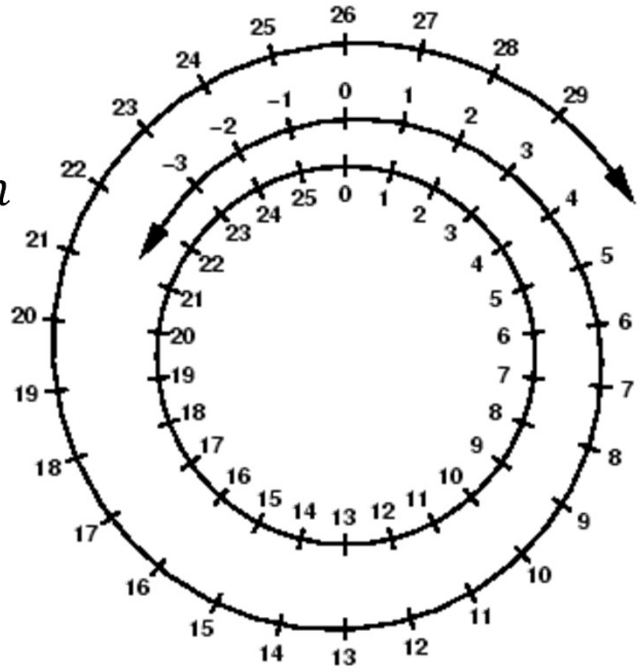
- Say $a = 17, n = 5$

- $17 mod \; 5 = 2$
- $(17 - 2) = 3 \times 5$ where $b = 2$ and $k = 3$



Modular Arithmetic monoalphabetic cipher

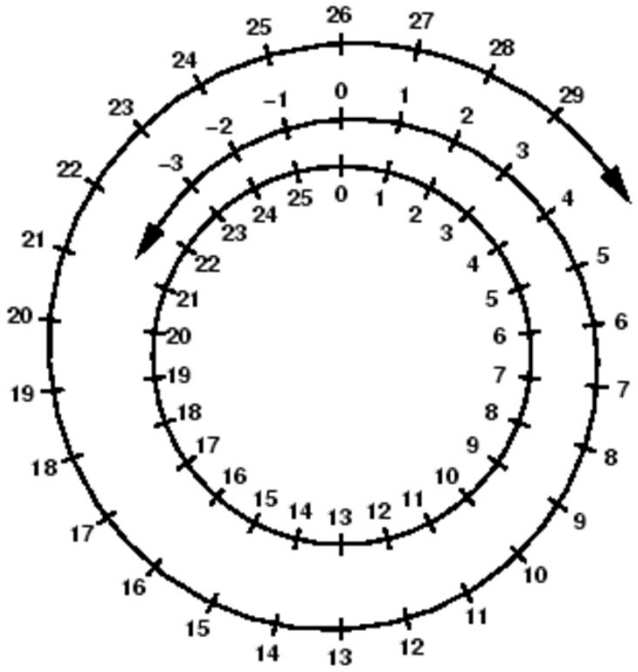
- $(a + b) \, mod \, n = ((a \, mod \, n) + (b \, mod \, n)) \, mod \, n$
- Say $a = 17, b = 3, n = 5$
- $\big((17 \, mod \, 5) + (3 \, mod \, 5)\big) mod \, 5$
- $= (2 + 3) mod \, 5 = 0$



Modular Arithmetic monoalphabetic cipher

- $(a \cdot b)\ mod\ n = ((a\ mod\ n) \cdot (b\ mod\ n))\ mod\ n$

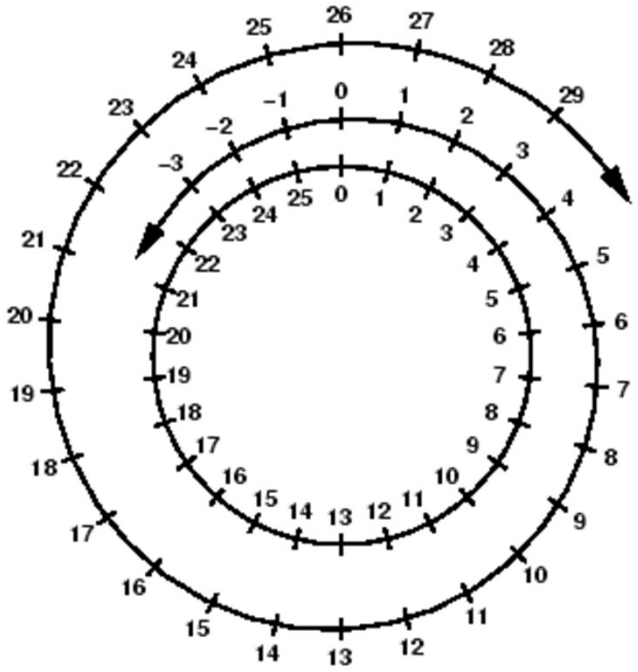
- Say $a = 17, b = 3, n = 5$
- $\big((17\ mod\ 5).(3\ mod\ 5)\big) mod\ 5 = (2 \times 3) mod\ 5 = 1$



Modular Arithmetic monoalphabetic cipher

- $-a \; mod \; n \; = \; n \; - \; (a \; mod \; n)$

- Say $a = 17, n = 5$
- $5 - (17 \; mod \; 5) = 5 - 2 = 3$



Cryptanalysis of the Caesar Cipher

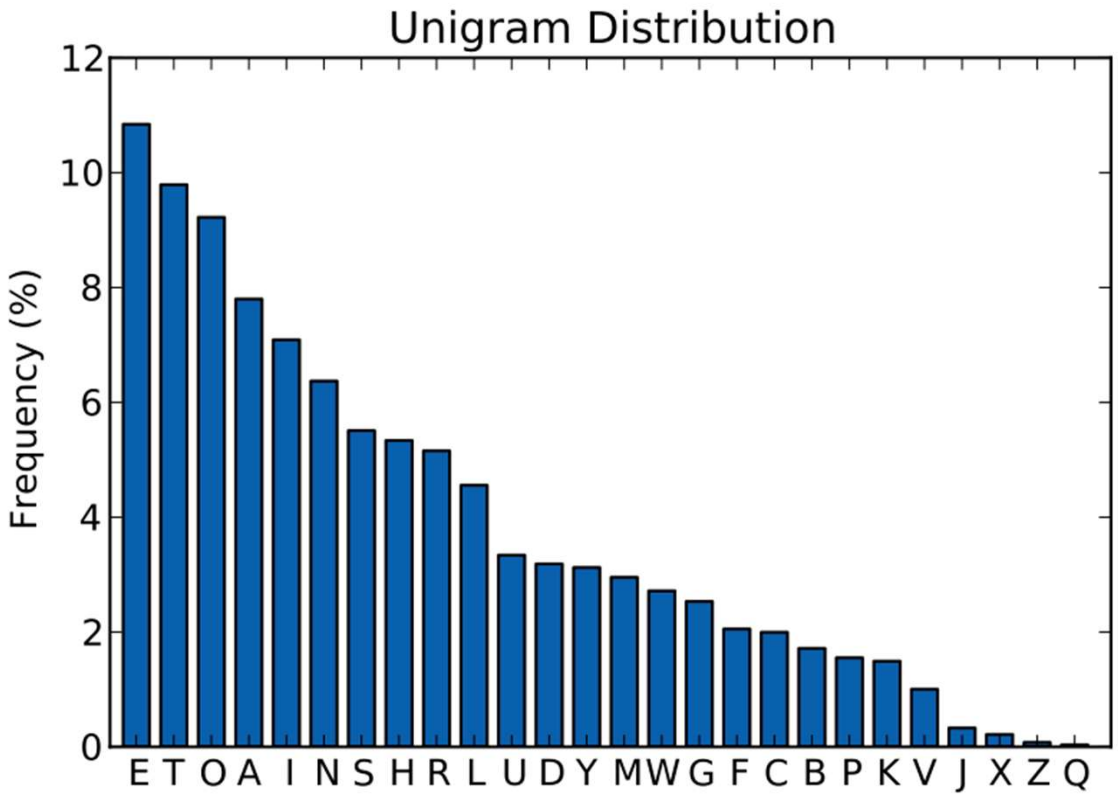
- only have 26 possible ciphers
- could simply try each in turn - exhaustive key search

Cryptanalysis of the Caesar Cipher

Single Letter	Double Letter	Triple Letter
E	TH	THE
T	HE	AND
R	IN	TIO
N	ER	ATI
I	RE	FOR
O	ON	THA
A	AN	TER
S	EN	RES

Character Frequencies

- in most languages' letters are not equally common
- in English e is by far the most common letter
- have tables of single double & triple letter frequencies



Affine Cipher

- transform each of the letter in plaintext to the corresponding integer in the range 0 to m-1 (m=26)
- Encryption $E(x) = (ax + b) \, mod \, m$
  - a and b are the key
- Say key $a = 5, b = 8$

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Affine Cipher

- Encryption $E(x) = (ax + b)\ mod\ m$
- key $a = 5$, $b = 8$

Plaintext	a	f	f	i	n	e		c	i	p	h	e	r
x	0	5	5	8	13	4		2	8	15	7	4	17
5x+8	8	33	33	48	73	28		18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2		18	22	5	17	2	15
Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P

Affine Cipher: Decryption

- Decryption $D(x) = c(x - b) \, mod \, m$
- c is the modular multiplicative inverse of a: $a \times c = 1 \, mod$
- key a = 5, b = 8
- $C = 21$
- since $21 \times 5 = 105 = 1 \, mod \, 26$
  - As 26 x 4 = 104, and 105 - 104 = 1

Affine Cipher: Decryption

- Decryption $D(x) = c(x - b) \, mod \, m$
- c is the modular multiplicative inverse of a: $a \times c = 1 \, mod$
- key a = 5, b = 8
- $C = 21$

Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P
y	8	7	7	22	21	2		18	22	5	17	2	15
21(y - 8)	0	-21	-21	294	273	-126		210	294	-63	189	-126	147
21(y - 8) mod 26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	a	f	f	i	n	e		c	i	p	h	e	r

Affine Cipher: Drawbacks

- key creates the situation where more than one plaintext letter is encrypted to the same ciphertext letter (for example, above both "e" and "r" encipher to "V")

- there is more than one number that can be multiplied by 4 to get 1 modulo 26.

- Solution: The inverse of a modulo m exists if and only if a and m are coprime $\gcd(a, m) = 1$

Affine Cipher: Drawbacks keys

- there are 12 numbers less than 26 which are coprime to 26
- for each of these there are 26 possibilities for the value of b
- total of 12 x 26 = 312 possible keys. Brute Force Attack!!!

Polyalphabetic Substitution

in general use more than one substitution alphabet

makes cryptanalysis harder since have more alphabets to guess

and because flattens frequency distribution

(since same plaintext letter gets replaced by several ciphertext letter, depending on which alphabet is used)

Vigenère Cipher

- basically multiple caesar ciphers
- key is multiple letters long K = k_(1) k_(2) ... k_(d)
- ith letter specifies ith alphabet to use
- use each alphabet in turn, repeating from start after d letters in message

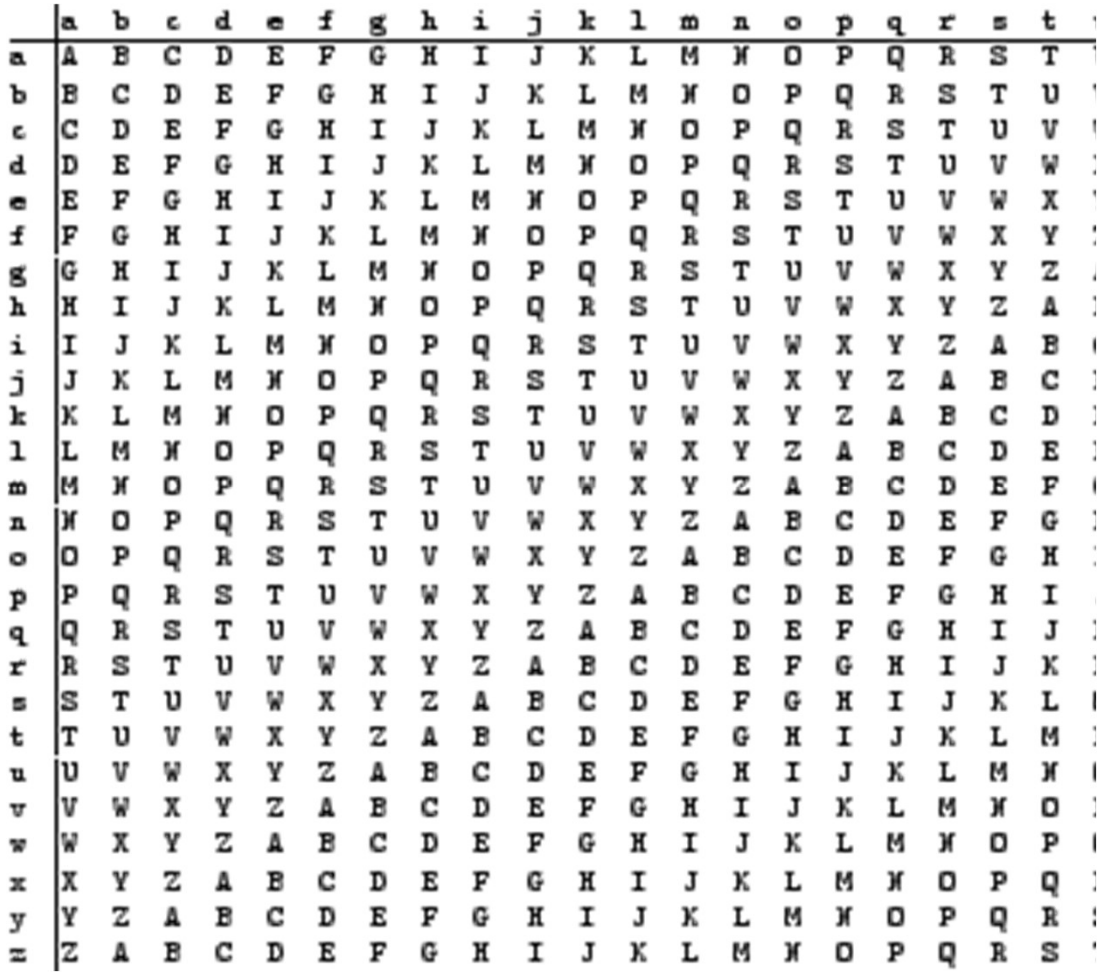
Many Caesars: the Vigenère Cipher

- Giovan Batista Belaso in 1553
- Key=jasmine (9, 0, 18, 12, 8, 13, 4)
- Plain text= we are getting hungry

	w	e	a	r	e	g	e	t	t	i	n	g	h	u	n	g	r	y
	22	4	0	17	4	6	4	19	19	8	13	6	7	20	13	6	17	24
+	9	0	18	12	8	13	4	9	0	18	12	8	13	8	4	9	0	18
=	5	4	18	3	12	19	8	2	19	0	25	14	20	2	17	15	17	16
	F	E	A	D	M	T	I	C	T	A	Z	O	U	C	R	P	R	Q

Vigenère Cipher: A tabula recta

- how people in the sixteenth century used the cipher
- 26 x 26 table listing all the shifts
- plaintext letter gives the row, and the key letter gives the column
- Apply numerical conversion and the modular addition



	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Kasiski examination

- For about 300 years, it was believed to be unbreakable until the 1920s
- Charles Babbage and Friedrich Kasiski independently determined a method of breaking it in the middle of the nineteenth century.
- repeated patterns in the text to determine the length of the key

Mixed Alphabets Cipher

- most generally we could use an arbitrary mixed (jumbled) alphabet
- each plaintext letter is given a different random ciphertext letter, hence key is 26 letters long

- Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
- Plaintext: IFWEWISHTOREPLACELETTERS
- Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

- now have a total of 26! keys

26! is secure !!

- brute force attack NOT possible!!
- problem is not the number of keys, rather:
  - there is lots of statistical information in message
  - can solve the problem piece by piece

(ie. can get key nearly right, and nearly get message, near enough MUST NOT be good enough!)

Cryptanalysis

use frequency counts to guess letter by letter

also have frequencies for digraphs & trigraphs

General Monoalphabetic: A special case of Mix Alphabets

- special form of mixed alphabet
- use key as follows:
  - write key (with repeated letters deleted)
  - then write all remaining letters in columns underneath
  - then read off by columns to get ciphertext equivalents
- Keyword: monoalphabetic
- second "o" is skipped as it has already appeared

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	M	O	N	A	L	P	H	B	E	T	I	C	D	F	G	J	K	Q	R	S	U	V	W	X	Y	Z

- "u" encrypts to "U", "v" to "V" and so on to "z". This problem occurs if the keyword does not contain any letters from near the end of the plaintext alphabet. To combat this problem, we can choose a keyword with a letter from near the end of the alphabet.

General Monoalphabetic: A special case of Mix Alphabets

- First we realise that there are 26 possible choices for the first letter in the ciphertext alphabet. Now, for the second letter, we can use any letter APART from the letter we have already selected for the first position, so there are 25 choices for the second position. For the third position we can choose any letter, apart from either the letter in the first position or the second position, and hence there are 24 choices here. Thus, for the first 3 places, there are 26 x 25 x 24 possible choices.

- Continuing in this way, we quickly find that there are 26!

Transposition Ciphers

Transposition Ciphers

- transposition or permutation ciphers hide the message contents by rearranging the order of the letters
- Scytale cipher
- an early Greek transposition cipher
- a strip of paper was wound round a staff
- message written along staff in rows, then paper removed
- leaving a strip of seemingly random letters
- not very secure as key was width of paper & staff

Scytale

- used by the Ancient Greeks and Spartans
- consisted of a polygonal rod or cylinder, around which was wrapped a piece of parchment.

Rail Fence cipher

write message with letters on alternate rows

read off cipher row by row

D		F		N		T		E		A		T		A		L
	E		E		D		H		E		S		W		L	

Plain: defend the east wall
Cipher: DFNTEATALEEDHESWL
Key=1

Rail Fence cipher

- Plain: defend the east wall
- Key=3
- Cipher: DNETLEEDHESWLXFTAAX

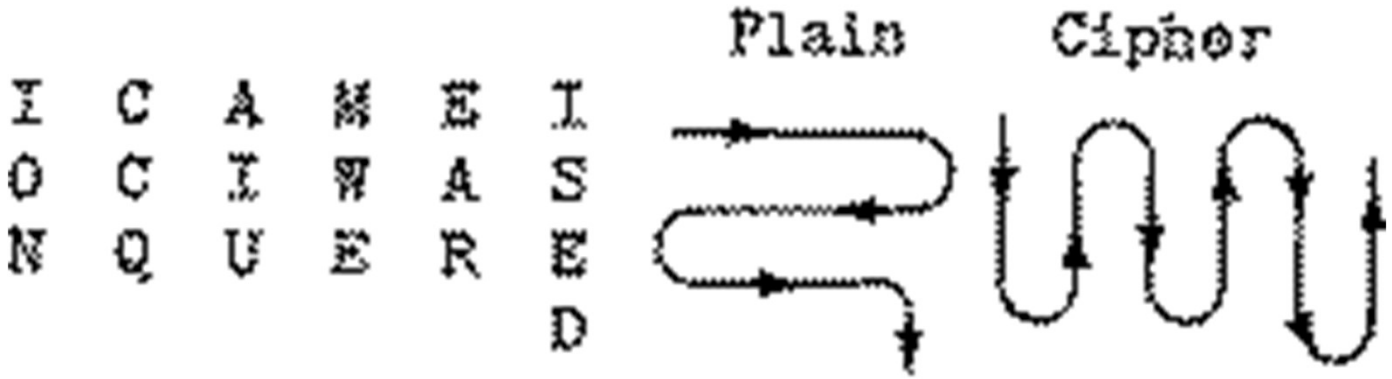
D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Rail Fence cipher

- limited number of usable keys, especially for short messages
- for there to be enough movement of letters, the length of the message needs to be at lease twice the key, but preferably 3 times the key
- The use of nulls can also have a detrimental effect on the security of the cipher, as an interceptor can use them to identify where the end of the line is, and so have a sensible guess at the key.
- Frequency Analysis

Geometric Figure/ Route Cipher

- write message following one pattern and read out with another



Cipher: IONQC CAIUE WMEAR DESI

Row Transposition ciphers

•in general write message in a number of columns and then use some rule to read off from these columns

•key could be a series of number being the order to: read off the cipher; or write in the plaintext

Plain: THESIMPLESTPOSSIBLETRANSPOSITIONSXX

Key (R): 2 5 4 1 3

Key (W): 4 1 5 3 2

T H E S I S T I E H M P L E S E M S L P T P O S S S T S O P I B L E T E I T L B R A N S P S R P N A O S I T I T O I I S O N S X X X O X S N

Cipher: STIEH EMSLP STSOP EITLB SRPNA TOIIS XOXSN